Transactions of the VŠB - Technical university of Ostrava Vol. VI, No. 2, 2011
Safety Engineering Series p. 27 - 31

EFFICIENCY EVALUATION OF PROTECTION SYSTEMS USING SOFTWARE SIMULATION

Juraj VACULÍK[1]

Research article

Abstract: Article describes the most common methods for evaluation of physical protection systems. It analyzes various software simulations and describes how mathematical model can be used for evaluation and designing of physical protection systems and how it can provide a basis for software simulation that could upgrade possibilities and extend the scope of previous software. Author is focusing on the selection of the best approaches from the evaluation of physical protection systems designed for nuclear facilities and how these approaches can be used in evaluation of physical protection systems designed for the protection of property, persons and tangible assets.

Key words: Efficiency of protection system, physical protection system, index of security measures, probability of interruption, protection system design.

Introduction

Protection system is a tool for the enforcement of a security policy (Reitšpís, 2004). One of the main responsibilities of protection system is to secure the system from violation of intruder. It is necessary to maximize the probability of intruder's detection in vital area and delay the intruder in the vital area as long as possible, so response force can move to the object and make intervention.

This article focuses on physical security, so we use the term physical protection system. This term is closely related to the protection of nuclear facilities (Loveček, 2004). Most of software simulation was made for evaluation of nuclear facilities.

However, we want to find the best developed approaches that can be used for the evaluating of systems that protect property, persons and tangible assets. Compared to nuclear facilities, these protection systems have different composition of security zones, so other techniques are necessary to fulfill the objectives.

The motivation for writing this article is to find the best approaches from existing mathematical models that can suit the modeling of systems used for the protection of various assets.

Materials and methods

Many studies have been carried out about the most often used methods, such as SAVI and ASSESS. In other cases we had to use limited sources, particularly for methods that are still in the development stage. For example, in the case of SATANO software, we used only the source code of application and one doctoral thesis related to this topic.

Because we based our research on existing particular solutions, the basic scientific method we used is the inductive generalization. We generalized various conclusions based on our particular findings.

Many times we also used method of comparison for comparing various approaches or we had to analyze various aspects in depth. Very common technique for the analyzing of security system is sensitivity analysis, because the exclusive usage of output parameters is very often difficult to interpret.

Results

During research, we analyzed various practical solutions that have been implemented in the past. As a review of our findings, we provide the analysis of various parameters and software simulations.

The most often used parameters for evaluation are:

- probability of interruption,
- probability of intruders elimination,
- index of security measures.

Basically, the index of security measures is a ratio between the shortest time of intruder's advance through vital area and the time of tactical unit intervention (Loveček, 2009). Probability of interruption is the probability that a response force will interrupt adversary before intruder’s task is completed (Jang, 2009) Probability of intruder’s elimination is the probability, that an intruder will be successfully eliminated by response force (Rybár, 2000).

[1] University of Žilina, Faculty of Special Engineering, Žilina, Slovakia, juraj.vaculik@fsi.uniza.sk

SATANO (Faculty of Special Engineering, University of Žilina)

Software SATANO implements four closely related models that were created together:

- Pragmatic model,
- Optimistic model,
- Pessimistic model,
- Realistic model.

The output of these models is the efficiency of protection system based on calculations of the index of security measures. Some of these models use the shortest path; others use the most probable path. Dijkstra algorithm is used for the calculation of the shortest path (Loveček, 2005).

These models are suitable for the calculation of the most probable time of physical protection system overcoming with the simulation of various types of situations, such as:

- Intruder has/doesn't have information about the shortest path,
- Background (visibility, traffic) is/isn't favorable.

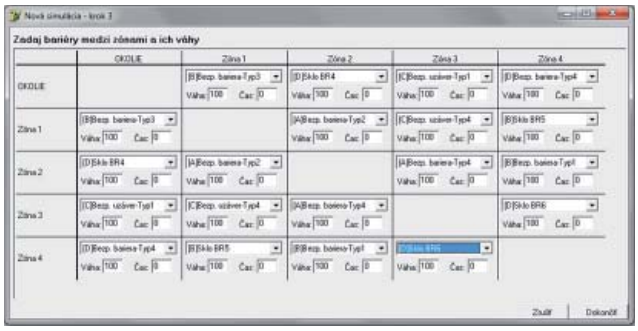

Fig. 1 Input matrix of GUI in SATANO

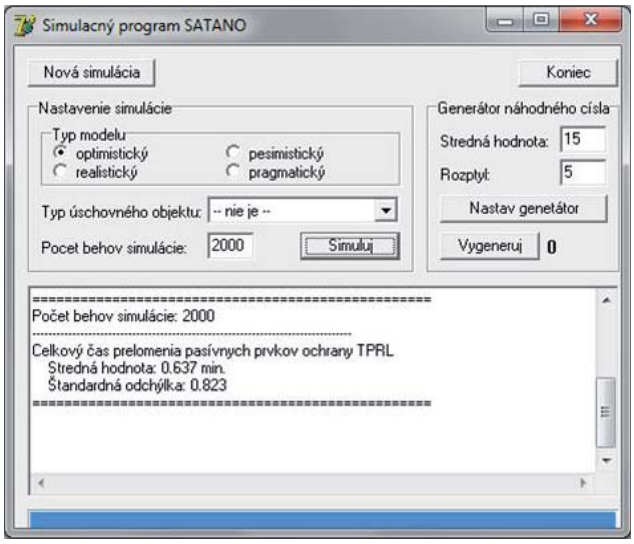

Fig. 2 GUI of SATANO

Input values can be defined as fixed values, normal distribution of probability can be used (Loveček, 2005). The matrix type of graphical user interface was used, so two different security zones could be connected only with a single join.

Such approach can be sometimes insufficient. For example, two rooms can be connected by several elements (wall, doors) and the selection of element with the lowest breaching endurance time can be tricky, because result can depend on the chosen set of intruder's tools.

EASI, ASD, SAVI (Sandia National Laboratories)

These three methods are based on the probability of interruption and they are intended for the evaluation of protection system security in nuclear facilities. They use central distribution of security zones. The intruder has all the information about security system (Phillips, 2004). The detection before critical point of detection is known as early detection.

EASI method (Estimation of Adversary Sequence Interruption) is used for the calculation of the probability of interruption on one (predefined) path.

In the graphical method called ASD, various layers are used for simulating the barriers that separate the intruder from his aim in the central zone.

SAVI method combines EASI and ASD methods and calculates the probability of interruption for all the paths to central zone and selects 10 most vulnerable zones. (SAVI, 1994) One component of SAVI is the database of the most often used barriers and detectors.

SAVI method implements also the analysis of sensitivity. RFT time is used as a basis for this analysis, because it is the most critical factor. The output is the probability of interruption. Figure 4 exhibits the sensitivity analysis for a path with the lowest probability of interruption.

Drawback of SAVI is the absence of probability of intruder's elimination.

ASSESS (Sandia National Laboratories)

ASSESS method (Analytic System and Software for Evaluating Safeguards and Security) is an enhanced method based on SAVI. Additional modules for the calculation of probability of external and internal intruder's elimination are used.

ASSESS also uses the probability of interruption and ASD method as basic methods (Phillips, 2004). ASSESS has also a new structure that consist of six independent modules.

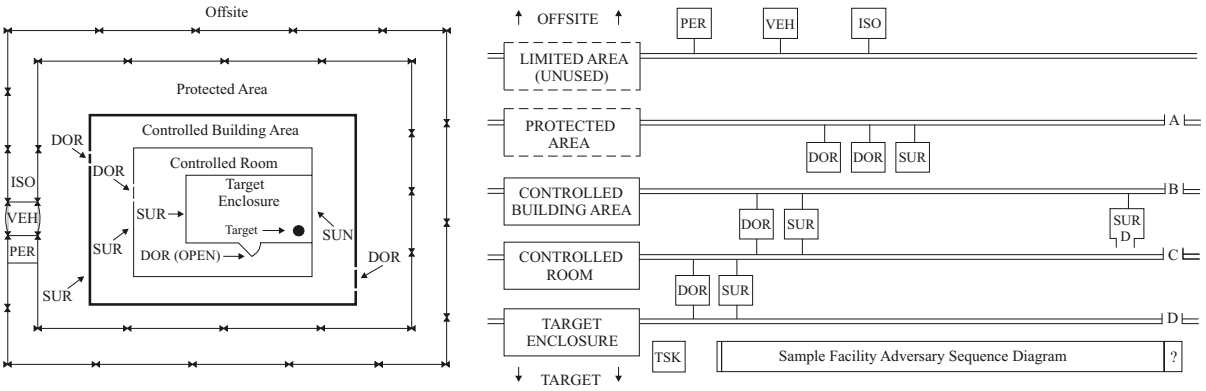

Fig. 3 Vital area (left) and application of ASD (right) (Analýza, 1991)

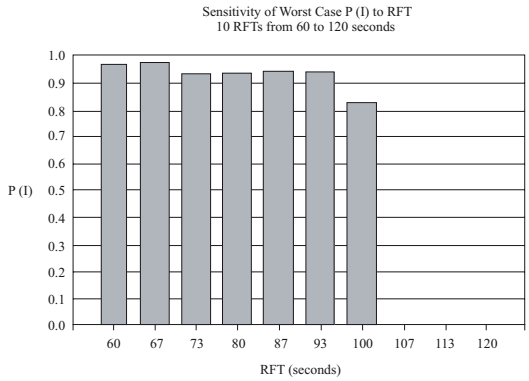

Fig. 4 Analysis of interruption (Analýza, 1991)

SAPE (Korea Institute of Nuclear Non-proliferation and Control)

SAPE (Systematic Analysis Of Physical Protection Effectiveness) is based on SAVI and ASSESS methods, but it has additional features. SAPE doesn't use ASD method, but 2D map instead.

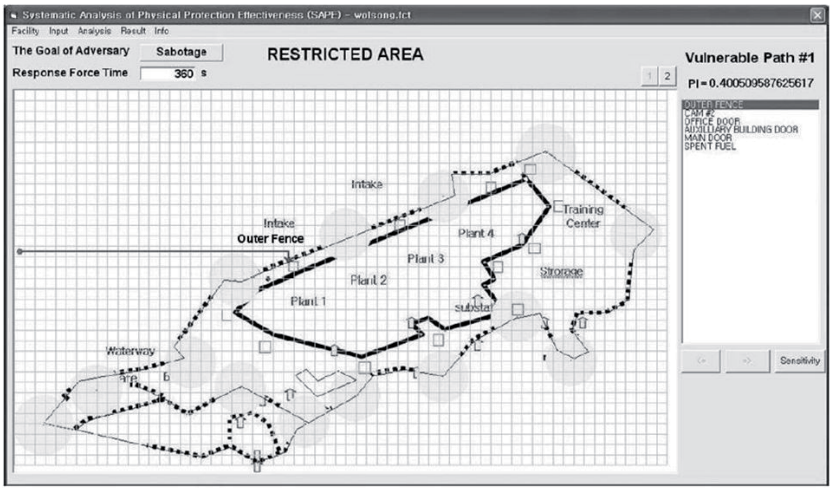

Fig. 5 2D maps used in SAPE (Jang, 2009)

Since ASD model is too simple to describe an arrangement of buildings, a facility map is required to imagine an adversary's path. This insufficient description also causes inaccuracies. The ASD cannot show at what point along a fence it has been penetrated, and the distance needed to cross an area is considered equal when using the ASD, regardless of the particular route (Jang, 2009).

2D map has the following advantages compared to an ASD:

- It provides intuitive bird's eye views of a physical protection system,
- It realistically represents the relative positions of protection elements (Jang, 2009).

SAPE uses another technique for sensitivity analysis. It is noted that SAVI shows a sensitivity graph of the probability of interruption according to response force time, while SAPE shows the sensitivity values to all protection elements located on a path.

This sensitivity represents relative upgrade efficiency, and hence higher sensitivity elements should be considered first for upgrade (Jang, 2009).

Discussion

We found out that the most often used output parameters can be used also for the purposes of property, tangible assets and personal protection systems. However underlying modeling techniques and the composition of security zones has to be changed, because centralistic distribution is not suitable.

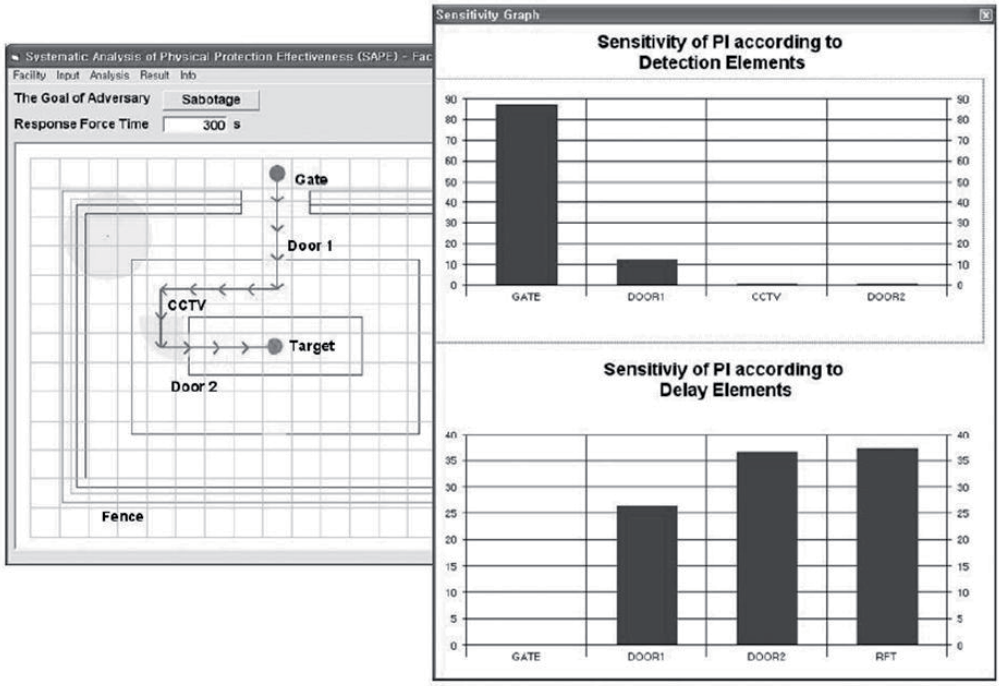

Fig. 6 Analysis of sensitivity in SAPE (Jang, 2009)

Main drawbacks of current methods can be divided into two groups:

- Problems with the model itself,
- Lack of input data.

Problems with the model depend on concrete model, but it is possible to formulate one common feature and that is the centralistic composition of models that is suitable for the evaluation of nuclear facilities but not suitable for property, persons and tangible assets protection systems.

Specific problem is the lack of input data that complicates the implementation of models. In systems for protection of property, persons and tangible assets, very wide group of detectors and barriers are used that enhance this problem.

Now we can define two main objectives of the modeling of physical protection system:

- to effectively design physical protection system (the most vulnerable paths through vital area will be effectively protected),
- to optimize financial costs spent on security, so various paths through vital area will be equally secured as long as there is the same amount of assets on various paths.

Method for evaluation can be fully-mathematical (method that will use path with the lowest probability of interruption) or can use virtual simulation with 3D model of object for finding the most probable intruder's path. Because both approaches have advantages and disadvantages, choosing the best approach should be based on additional scientific research on this topic.

Current methods prefer fully-mathematical modeling, but perhaps only because of limited opportunities of realistic modeling using virtual reality in times when the methods were created (some methods are dating back to the 70s and 80s).

Finding of the most probable path through vital area could be the preferred way because the securing of the most probable path is crucial. On the other hand, other (less probable paths) could remain deficiently secured.

Conclusion

Based on analysis, we can conclude some important points. Above all, the existing models are not suitable for protection systems, that are not designed for protecting of nuclear facilities or similar objects (that use one central zone). Method that can evaluate systems with many security zones with protected assets is needed, but this method can be based on existing techniques, such as probability of interruption or index of security measures.

Important step in the usage of method in practice is to fill databases of breaching endurance times of various barriers from different vendors. The complexity of this problem is the main obstacle for further development and specialized studies need to be carried out. The method for the estimation of detection probability needs to be created.

References

A Risk Assessment Methodology (RAM) for Physical Security. (2005). Sandia Corporation, White Paper.

Analýza účinnosti systému bezpečnostní ochrany jaderných zařízení a jadrných materiálu. (1991). Ústav jaderných informácí.

JANG, S. (2009). Development of a Vulnerability Assessment Code for a Physical Protection System : Systematic Analysis of Physical Protection (SAPE). *Nuclear Engineering and Technology*, Vol. 41, No. 5, 2009.

LOVEČEK, T. (2005). *Hodnotenie kvality bezpečnostných systémov*. [Dizertačná práca]. Žilina.

LOVEČEK, T. (2009). *Systémy ochrany majetku a možnosti ich kvalitatívneho a kvantitatívneho ohodnotenia*. [Habilitačná práca]. Žilina.

PHILLIPS, G. (2004). *New Vulnerability Assessment Technologies vs the Old VA Tools*. New Meets Old. National Security Program Office.

Physical Protection of Nuclear Facilities and Materials, Albuquerque, New Mexico, USA.

REITŠPÍS, J. (2004). *Manžérstvo bezpečnostných rizík*. Žilina: Edis, 2004. 296 s. ISBN 80-8070-328-0.

RYBÁR, M. (2000). *Modelovanie a simulácia vo vojenstve*. Bratislava: Vydavateľská a informačná agentúra, Ministerstvo obrany Slovenskej republiky, 2000. ISBN 80-88842-34-4.

SAVI 4.0 (1994). Reference manual, internal document, Sandia National Laboratories, 1994.